

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,)	Case No. 1:22-cr-615
)	
Plaintiff,)	Judge J. Philip Calabrese
)	
v.)	Magistrate Judge
)	Jonathan D. Greenberg
LAWRENCE STURDIVANT,)	
)	
Defendant.)	
)	

OPINION AND ORDER

On October 27, 2022, a federal grand jury charged Defendant Lawrence Sturdivant with multiple counts of robbery, attempted robbery, and brandishing a firearm during and in relation to a crime of violence. Defendant moves to suppress all evidence stemming from law enforcement's warrantless search of automatic license plate reader databases during the investigation of the robberies. This motion presents a close and difficult constitutional question where the Fourth Amendment meets a new and emerging technology. For the following reasons, the Court **DENIES** the motion.

BACKGROUND

This case arises from an investigation into ten robberies that occurred in the Cleveland, Ohio area between December 5, 2021 and December 26, 2021.

A. The Robberies

On December 5, 2021, a man walked into a Walgreens store, pointed a gun at the cashier, and took handfuls of bills out of the register. (ECF No. 1-1, ¶¶ 8-9,

PageID #5.) Witnesses and store surveillance video indicated that the suspect was a black male of tall, slender build wearing dark clothing and gloves who escaped in a black sedan. (*Id.*) About half an hour later, a man matching that description robbed a second Walgreens a few miles away. (*Id.*, ¶¶ 10–13, PageID #6–7.)

On December 11, 2021, a man entered a Family Dollar store, pointed a gun at employees, and told them to open the cash register but became impatient when they were unable to do so and left the store empty-handed. (*Id.*, ¶¶ 15–17, PageID #7.) Witnesses described the suspect as a black male wearing a black facemask, a navy-blue jacket, gray sweatpants, and gloves, who arrived at the store in a new black Chevrolet Camaro with tinted windows and silver rims. (*Id.*, ¶¶ 16 & 18, PageID #7–8.) About forty minutes later, a man matching that description robbed a second Family Dollar about twelve miles away. (*Id.*, ¶¶ 19–21, PageID #8.)

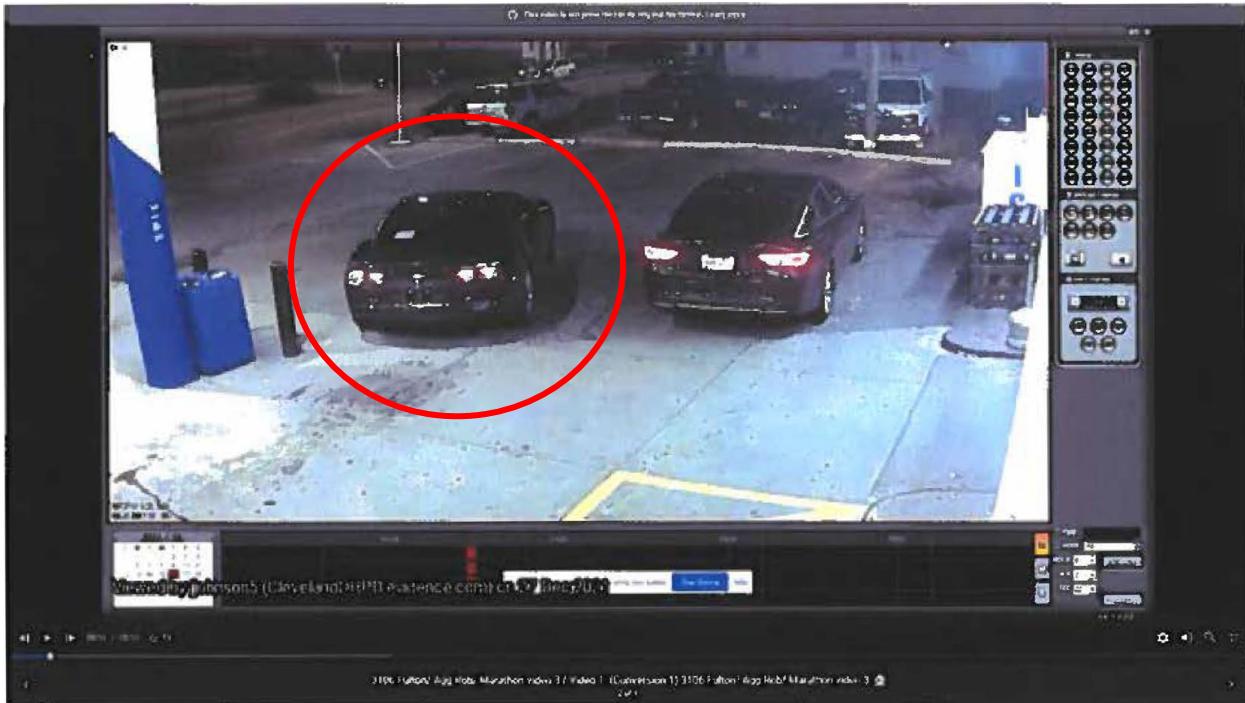
On December 16, 2021, a man entered a Walgreens, pointed a gun at the cashier, and grabbed money out of the cash register. (*Id.*, ¶¶ 23–24, PageID #9.) Witnesses described the suspect as a skinny black male approximately six feet tall wearing black clothing and a black facemask who fled in a dark-colored sedan. (*Id.*, ¶¶ 23–25, PageID #9–10.) About fifty minutes later, a man matching the same description robbed a CVS about six miles away. (*Id.*, ¶¶ 28–29, PageID #11–12.) Surveillance video showed the suspect fleeing in a black Chevrolet Camaro. (*Id.*, ¶ 30, PageID #12.)

On December 18, 2021, a man entered a Family Dollar store, presented a gun, and demanded the money from the cash register. (*Id.*, ¶¶ 31–32, PageID #12–13.)

Witnesses described him as a thin black male approximately six feet tall wearing black clothing and a facemask. (*Id.*, ¶ 32, PageID #12–13.) On December 26, 2021, a man matching that description and wearing similar clothing robbed three other Family Dollar stores in the same area. (*Id.*, ¶¶ 34–40, PageID #13–15.) Surveillance video footage showed a black Chevrolet Camaro with black custom rims near the location of the first of these robberies, a man matching the suspect’s description exiting the vehicle, and the man returning to the vehicle just after the store reported the robbery. (*Id.*, ¶ 35, PageID #14.)

B. The Investigation

By examining surveillance video footage from the December 16, 2021 Walgreens robbery, the Cleveland police identified the suspect’s vehicle as a black Chevrolet Camaro with a temporary license plate hanging in the rear window and a black-and-white bumper sticker on the lower right side of the rear bumper. (*Id.*, ¶ 27, PageID #11.) Surveillance footage from a nearby gas station showed the same suspect vehicle:



(ECF No. 1-1, ¶ 27, PageID #11; ECF No. 92-12, ¶ 14, PageID #1113; ECF No. 92, PageID #621; ECF No. 93, PageID #1354; ECF No. 98, PageID #1879; ECF No. 97, PageID #1696.) However, law enforcement was unable to make out the license plate number from the footage. (ECF No. 1-1, ¶ 27, PageID #11; ECF No. 92-12, ¶ 14, PageID #1113.)

On December 20, 2025, Special Agent Nathan E. Schwartz with the Bureau of Alcohol, Tobacco, Firearms and Explosives began investigating this series of robberies. (ECF No. 1-1, ¶ 41, PageID #16; ECF No. 97, PageID #1699; ECF No. 98, PageID #1882.) To locate the suspect vehicle, Special Agent Schwartz enlisted the help of Michael Thrush, an ATF Industry Operation Intelligence Specialist. (ECF No. 1-1, ¶ 41, PageID #16; ECF No. 97, PageID #1699; ECF No. 98, PageID #1882.) Thrush searched a database that used data from two automatic license plate reader systems, Flock Safety and ELSAG, for vehicles matching the suspect vehicle's

description. (ECF No. 1-1, ¶ 41, PageID #16; ECF No. 92-12, ¶ 23, PageID #1115–16; ECF No. 97, PageID #1699; ECF No. 98, PageID #1882.)

Automatic license plate readers are cameras specialized for capturing images of license plates from passing vehicles. (ECF No. 92-3, PageID #813; David J. Roberts & Meghann Casanova, *Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement* 9 (2012) (attached as Appendix A).) These systems use analytic software to associate license plate numbers with the date, time, and location of each vehicle that passes a camera. (ECF No. 92-3, PageID #813–14; Roberts & Casanova at 10.) Users can query an ALPR system for a certain license plate number and receive images containing those license plates. The extensive record in this case shows the following facts about the automatic license plate readers at issue.

B.1. Flock Safety

Most local police departments in Cuyahoga County have contracts with Flock Safety, a private ALPR provider that leases access to its cameras to law enforcement agencies. (ECF No. 92-1.) Flock customers can choose to share their data with other customers, forming a network of cameras across multiple customers and jurisdictions nationwide. (*FlockOS*, Flock Safety, <https://www.flocksafety.com/flock-os> [<https://perma.cc/KQN9-THFH>] (last visited June 9, 2025) (attached as Appendix B).) As a result, law enforcement customers have access to all Flock cameras that opt into the network, not just the cameras they lease. (*Frequently Asked Questions—Software*, Flock Safety, <https://www.flocksafety.com/faq#software> [<https://perma.cc/9GH8-29CK>] (last visited June 9, 2025) (attached as Appendix C).)

There are 1,636 Flock cameras across Cuyahoga County, 667 of which are associated with law enforcement agencies. (ECF No. 92-1; ECF No. 92-7; ECF No. 92-8; ECF No. 92-9; ECF No. 92-10, PageID #961–62.) Flock retains images from these cameras for thirty days. (*Frequently Asked Questions—Privacy and Access*, Flock Safety, <https://www.flocksafety.com/faq#privacy> [<https://perma.cc/VHH4-SNSG>] (last visited June 9, 2025) (attached as Appendix D).)

Flock provides a cloud-based software platform on which law enforcement can search through photographs taken by cameras in the network. (Appendix B.) Like many ALPR systems, the Flock platform allows law enforcement to search for license plate numbers and receive photographs containing them. (*Id.*; ECF No. 97-2.) However, images from Flock cameras extend well beyond just the license plate of a car, capturing the whole vehicle and its surroundings. (See, e.g., ECF No. 1-1, PageID #17; ECF No. 97-1, PageID #1747.) In addition to license plate numbers, Flock can identify vehicle characteristics such as color, body type, make and model, damage, temporary tags, and alterations like roof racks and after-market wheels. (*Frequently Asked Questions—Camera*, Flock Safety, <https://www.flocksafety.com/faq#camera> [<https://perma.cc/CR8A-3GHR>] (last visited June 9, 2025) (attached as Appendix E); ECF No. 97-2.) This capability allows law enforcement to begin with only a physical description of a vehicle and then figure out its license plate number.

B.2. ELSAG

The second camera network involved in this investigation is the ELSAG system, provided by Selex ES, a subsidiary of Leonardo S.p.A. (ECF No. 92-3; ECF No. 92-4.) The Cuyahoga County Sheriff's Office established this network, which the

Chagrin Valley Dispatch hosts to coordinate first responders in Northeast Ohio. (ECF No. 92-2; ECF No. 92-3.) At oral argument, both parties agreed that, on this record, there was no legally significant difference between the Flock and ELSAG systems.

Like the Flock system, the ELSAG system is a network of ALPR cameras capturing images that law enforcement can search by license plate number or by vehicle characteristics. (ECF No. 92-3, PageID #813; *see, e.g.*, ECF No. 92-11, PageID #980.) Like the Flock network, the ELSAG network incorporates cameras from law enforcement and private customers in the county and in various other political subdivisions. (ECF No. 92-3; ECF No. 92, PageID #617–18; ECF No. 93, PageID #1351–52; ECF No. 92-5.) Chagrin Valley Dispatch accesses approximately 1,119 cameras in the greater Cleveland metropolitan area when it runs a search through this system. (ECF No. 92-10; ECF No. 92, PageID #619; ECF No. 93, PageID #1352.) ELSAG cameras can capture at least nine hundred plates per minute, and the database retains all images for one year. (ECF No. 92-6, PageID #865–66; ECF No. 92-3, PageID #813.)

B.3. Use of ALPRs in This Investigation

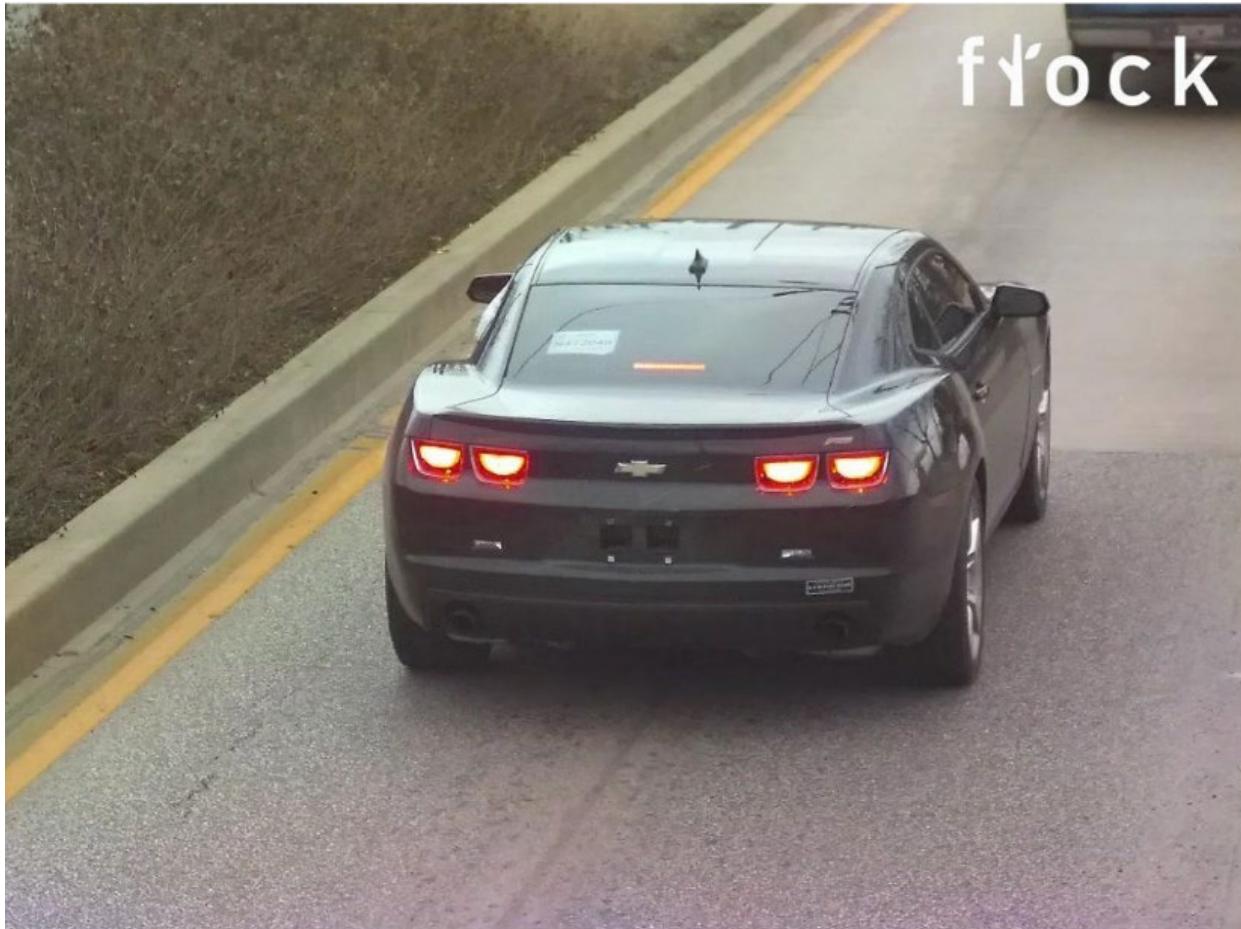
To find the suspect vehicle in this case, Thrush, the ATF Industry Operation Intelligence Specialist, searched the Flock and ELSAG databases for a black Chevrolet coupe with a temporary license tag and bumper sticker using the conventional surveillance image above. (ECF No. 1-1, ¶ 42, PageID #16; ECF No. 92-12, ¶ 23, PageID #1115–16; ECF No. 97, PageID #1701; ECF No. 98, PageID #1884.) Specifically, local police departments in Highland Heights, Newburgh

Heights, and Brooklyn, Ohio as well as the Chagrin Valley Dispatch were associated with the automatic license plate reader database searches relevant to this case. With the suspect vehicle blown up, that image from December 16, 2021 appears as follows:



(ECF No. 1-1, ¶ 42, PageID #17; ECF No. 92-12, PageID #1117.) Thrush ran queries such as “Black All Images Temporary Tag Ohio Tennessee Georgia Indiana,” “Chevrolet Black All Images,” and “Black No Plates.” (ECF No. 92-13, PageID #1189–90.)

Along with an unknown number of other search results, the Flock system yielded a photograph of a black Chevrolet Camaro with a temporary license tag in the rear window and a black-and-white bumper sticker on the rear right bumper:



Newburgh Heights OH PD -#02 Harvard Ave Westbound

12/16/2021 11:02:36 EST

(ECF No. 1-1, ¶ 42, PageID #16–17; ECF No. 92-12, ¶ 24, PageID #1117.) The Flock photograph placed this vehicle within about a fifteen-minute drive of the two robberies that occurred on December 16, 2021, about three hours after the robberies occurred. (See ECF No. 1-1, ¶ 42, PageID #16.) Unlike the surveillance footage, the Flock photograph did capture a discernable temporary license plate number. (*Id.*)

Using this license plate number, Thrush searched the National Crime Information Center system and found the vehicle's year, make, model and vehicle identification number. (*Id.*, ¶ 43, PageID #18.) He also learned that the vehicle was registered to Mr. Sturdivant. (*Id.*)

Armed with Mr. Sturdivant's name, law enforcement discovered that he matched the physical description of the suspect, had a previous conviction for aggravated robbery in 2014, and had been on active parole for that conviction since May 2021. (*Id.*, ¶¶ 43–44, PageID #18.) Special Agent Schwartz relayed this information to the Cleveland police detective investigating the case, who contacted Mr. Sturdivant's parole officer. (*Id.*, ¶¶ 45–46, PageID #18.) Mr. Sturdivant's parole officer advised that Mr. Sturdivant worked at Chipotle—witnesses at two of the robberies stated that the suspect wore a Chipotle-branded hat—and that he reported on December 9, 2021 that he had bought a black Chevrolet Camaro. (*Id.*, ¶ 46, PageID #18–19.)

C. Mr. Sturdivant's Stolen Vehicle Report

On or before December 26, 2021, the day of the last robberies, the Cleveland police attempted to stop a black Chevrolet Camaro because they were aware that it was the type of car involved in the robberies. (ECF No. 1-1, ¶ 48, PageID #19; ECF No. 97, PageID #1704 n.5.) However, the vehicle fled before the officers could complete the stop. (ECF No. 1-1, ¶ 48, PageID #19.) During the attempted stop, officers did not identify Mr. Sturdivant or his car, and the officers did not write a report because they did not complete the stop. (*Id.*; ECF No. 102-2, PageID #1939.) It is unknown whether those officers were aware of the license plate number resulting from the searches of the automatic license plate reader databases. (ECF No. 102-2, PageID #1939.)

On December 26, 2021, around 10:06 p.m., Mr. Sturdivant contacted the Cleveland police to report that his vehicle was stolen earlier that morning. (ECF

No. 1-1, ¶ 47, PageID #19.) He stated that he did not call in the morning because he wanted to “handle it in the streets.” (*Id.*) The responding officers toured the area and were unable to locate Mr. Sturdivant. (*Id.*) A few hours later, at around 12:45 a.m. on December 27, 2021, officers located a black Chevrolet Camaro with the license plate and VIN numbers of the suspect vehicle. (*Id.*, ¶ 49, PageID #19.) A witness reported that a 5’11” black male with a thin build wearing a black jacket parked the vehicle, then walked away. (*Id.*, PageID #19–20.) Special Agent Schwartz obtained surveillance video footage from the area because he learned that Mr. Sturdivant’s girlfriend lived on the street where officers found the vehicle. (*Id.*, ¶ 50, PageID #20.) The footage showed Mr. Sturdivant pulling the vehicle into the driveway of an apparently vacant house near his girlfriend’s home, cleaning the vehicle, driving the vehicle toward the location where officers eventually found it, and then walking back to his girlfriend’s home. (*Id.*)

D. Arrest and Further Investigation

On December 29, 2021, Mr. Sturdivant was arrested on State-issued warrants. (ECF No. 1-1, ¶ 51, PageID #20.) Federal agents obtained a search warrant for his cell phone records and location data. (*Id.*, ¶ 52, PageID #20–21.) By analyzing his cell-site location information along with surveillance footage and ALPR data, law enforcement associated Mr. Sturdivant’s movements with the robberies and the black Chevrolet Camaro. (*Id.*, ¶¶ 54–58, PageID #21–23.) At some point, Special Agent Schwartz created a 131-slide PowerPoint timeline of the investigation’s findings regarding Mr. Sturdivant’s movements, compiling in chronological order ALPR reports, still images from conventional security camera footage, photographs of the

robbed stores, and maps visualizing cell phone location information. (ECF No. 92-11; ECF No. 97, PageID #1691–92 n.2; ECF No. 97-1; ECF No. 98, PageID #1874–75 n.2.) Eleven photographs from Flock and eleven photographs from ELSAG appear in the slideshow, each showing Mr. Sturdivant’s car traveling along a public road and each tagged with the date, time, and location. (ECF No. 92-11; ECF No. 97-1.) During discovery, the United States turned over an additional four ELSAG reports that do not appear in the slideshow. (ECF No. 92-17.) In total, the record contains 26 unique ALPR photographs of Mr. Sturdivant’s car between November 13, 2021 and December 26, 2021, each timestamped and geotagged.

STATEMENT OF THE CASE

On October 27, 2022, a federal grand jury indicted Mr. Sturdivant for ten counts of interference and attempted interference with commerce by robbery in violation of 18 U.S.C. § 1951(a), three counts of using, carrying, and brandishing a firearm during and in relation to a crime of violence in violation of 18 U.S.C. § 924(c)(1)(A)(ii), and one count of being a felon in possession of ammunition in violation of 18 U.S.C. §§ 922(g)(1) & 924(a)(2). (ECF No. 20.)

Defendant moves to suppress evidence from the searches of automatic license plate reader databases, arguing that their use in this case constitutes a search under the Fourth Amendment. Because law enforcement did not obtain a warrant before conducting these searches, Defendant contends, they violated the Fourth Amendment. Therefore, the Court must exclude any evidence they produced. The

United States responds that queries of ALPR databases do not constitute searches under the Fourth Amendment.

ANALYSIS

The Fourth Amendment protects the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. Further, it provides that “no Warrants shall issue but upon probable cause supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” *Id.*

Although the record in this case would appear to provide probable cause for a warrant to search the Flock and ELSAG databases, no investigator sought or obtained one. In circumstances like those in this investigation, where time was not of the essence, obtaining a warrant would be prudent and the best practice, even if not constitutionally required. In the absence of a warrant, the Court turns to the competing lines of authority that have emerged under the Fourth Amendment to evaluate whether querying the ALPR databases constitutes a search and, if so, its reasonableness.

I. Fourth Amendment Jurisprudence

Historically, courts looked to the common law of trespass to determine whether a search implicating the Fourth Amendment occurred. *Carpenter v. United States*, 585 U.S. 296, 304 (2018). Under this approach, a Fourth Amendment search occurs where “the Government ‘obtains information by physically intruding on a constitutionally protected area.’” *Id.* (quoting *United States v. Jones*, 565 U.S. 400, 406 n.3 (2012)).

More recently, however, the Supreme Court recognized that “property rights are not the sole measure of Fourth Amendment violations.” *Id.* (quoting *Soldal v. Cook County*, 506 U.S. 56, 64 (1992)). “[T]he Fourth Amendment protects people, not places.” *Katz v. United States*, 389 U.S. 347, 351 (1967). Tracing to the second Justice Harlan’s concurrence in *Katz*, this view “expanded our conception of the Amendment to protect certain expectations of privacy as well.” *Carpenter*, 585 U.S. at 304. In this view, where (1) an individual exhibits an actual, subjective expectation of privacy by seeking to preserve something as private and (2) the expectation is one that society is prepared to recognize as reasonable—in other words, one that is objectively justifiable under the circumstances—the Fourth Amendment will protect that expectation against government invasion. *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

Over time, the reasonable-expectation-of-privacy standard produced several lines of Fourth Amendment doctrine. ALPR data sits at the intersection of two such bodies of jurisprudence, each pointing in a different direction. On the one hand, a car’s license plate and exterior appearance belong to a category of vehicle-related identification in which an individual has no reasonable privacy interest. On the other hand, the ability to track drivers continuously and retroactively raises the specter of a surveillance state.

I.A. License Plates and Exterior Characteristics of Vehicles

Under the Fourth Amendment, there is “no reasonable expectation of privacy in the information contained on [a] license plate.” *United States v. Ellison*, 462 F.3d 557, 561 (6th Cir. 2006). This rule derives from the plain view doctrine, which holds

that the “seizure of property in plain view involves no invasion of privacy and is presumptively reasonable.” *Texas v. Brown*, 460 U.S. 730, 738 (1983). Where an object sits in the “plain view” of an officer who is in a place lawfully, the object’s owner no longer has a privacy interest in that object; his “remaining interests in the object are merely those of possession and ownership.” *Id.* at 739. Further, expectations of privacy in one’s car are especially low because a car “seldom serves as one’s residence or as the repository of personal effects,” is subject to “pervasive and continuing governmental regulation and controls,” and “has little capacity for escaping public scrutiny” as it “travels public thoroughfares where both its occupants and its contents are in plain view.” *New York v. Class*, 475 U.S. 106, 112–13 (1986) (citations omitted).

Applying these principles, the Supreme Court held that a vehicle identification number located inside the passenger compartment but visible outside the car does not receive Fourth Amendment protection. *Id.* at 113–14. Subjectively, motorists should expect that officers may access vehicle identification numbers because they play “an important part in the pervasive regulation by the government of the automobile.” *Id.* at 113. Objectively, “it is unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile.” *Id.* at 114. Despite its location inside a car, the “mandated visibility” of the vehicle identification number likens it to the car’s exterior, which, “of course, is thrust into the public eye, and thus to examine it does not constitute a ‘search.’” *Id.*

“Logically, this reasoning extends to a legally-required identifier located *outside* the vehicle.” *Ellison*, 462 F.3d at 561. Accordingly, the Sixth Circuit holds that there is no reasonable expectation of privacy in one’s license plate number either. *Id.* Like vehicle identification numbers, license plate numbers also play an important role in the pervasive government regulation of the automobile, which includes rules mandating their visibility. “The very purpose of a license plate number, like that of a Vehicle Identification Number, is to provide identifying information to law enforcement officials and others.” *Id.*

In *Ellison*, the absence of a privacy interest in one’s license plate number meant that a search within the meaning of the Fourth Amendment did not occur where a police officer entered that number into a law-enforcement database, which returned information that the car was registered to a man with an outstanding felony warrant. *Id.* at 562–63. Such technology “does not allow officers to access any previously-unobtainable information; it simply allows them to access information more quickly.” *Id.* at 562. Because officers obtained the license plate number without intruding on a constitutionally protected area, “there was no ‘search’ for Fourth Amendment purposes.” *Id.* at 563.

Overall, queries of automatic license plate reader databases present, at most, only a marginal extension of *Ellison* and its predecessors. Under this line of authority, Mr. Sturdivant has no reasonable expectation of privacy in the exterior appearance of his car or its temporary license plate. Subjectively, he should expect others, including law enforcement, to see his license plate number and the exterior

appearance of his car. Objectively, it is not reasonable to have an expectation of privacy in a license plate or temporary tag, which the law requires to be visible on the outside of a car. Therefore, he has no privacy interest in the ALPR search results either, which produced photographs and images of the car's exterior and used them to identify the suspect vehicle and its owner. As previously noted, this conclusion stands in some tension with another line of cases, to which the Court turns next.

I.B. Surveillance

The Fourth Amendment “seeks to secure ‘the privacies of life’ against ‘arbitrary power.’” *Carpenter*, 585 U.S. at 305 (quoting *Boyd v. United States*, 116 U. S. 616, 630 (1886)). In doing so, the Founders aimed “to place obstacles in the way of a too permeating police surveillance.” *United States v. Di Re*, 332 U. S. 581, 595 (1948). As technology enhances the government’s “capacity to encroach upon areas normally guarded from inquisitive eyes,” courts must “assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Kyllo v. United States*, 553 U.S. 27, 34 (2001).

In *Carpenter*, these principles led the Supreme Court to reject the warrantless acquisition of historical cell-site location information from a defendant’s cell-service providers. Cell-site location information is the time-stamped record that a cell phone generates each time it connects to a cell tower or other radio antennas that provide service. *Carpenter*, 585 U.S. at 300. “Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone’s features.” *Id.* at 300–01. The precision of this information depends on the size of the geographic area that the cell site covers.

Id. at 301. As data usage grows, wireless carriers install more cell sites, leading to increasingly compact coverage areas and increasingly precise cell-site location information. *Id.*

In *Carpenter*, the data at issue placed the defendant “within a wedge-shaped sector ranging from one-eighth to four square miles.” *Id.* at 312. Investigators obtained 127 days of historical cell-site location information from one provider and two days from another, totaling 12,898 points of location data for an average of 101 data points per day. *Id.* at 302. Based on this data, law enforcement placed the defendant at or near various robberies for which they arrested and charged him. *Id.* at 301–03.

Although an individual would not necessarily enjoy Fourth Amendment protection from being observed by an officer in a public place, the Supreme Court held that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI,” whether the government uses its own technology or relies on that of a third party. *Id.* at 310. This holding built on earlier decisions in which members of the Supreme Court recognized that individuals have a reasonable expectation of privacy “in the whole of their physical movements.” *Id.* (citations omitted). At bottom, the “detailed, encyclopedic, and effortlessly compiled” nature of historical cell-site location information troubled the Court and presented a “qualitatively different” type of privacy interest to guard against governmental intrusion. *Id.* at 309. “Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch,” but doing so for any extended period of

time was cost prohibitive and, therefore, rare. *Id.* at 310. Accordingly, “society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.” *Id.* (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment)). In contrast, cell phone tracking offered a “remarkably easy, cheap, and efficient” way to assemble “an all-encompassing record of the holder’s whereabouts.” *Id.* at 311. Such a record has the potential to open “an intimate window into a person’s life,” revealing not only physical movements but, through them, “familial, political, professional, religious, and sexual associations.” *Id.* (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

Further, the Court emphasized the retrospective nature of historical cell-site location information. Because they acquire data regarding a suspect’s past movements, “police need not even know in advance whether they want to follow a particular individual, or when.” *Id.* at 312. Instead, the government was in effect running constant, granular surveillance against every cell phone owner, the results of which it could call upon at its discretion. *Id.* This “retrospective quality of [historical cell-site location information] gives police access to a category of information otherwise unknowable”—the movements of individuals before they come to the attention of law enforcement. *Id.*

In short, the Supreme Court “decline[d] to grant the state unrestricted access” to a database of individuals’ historical location information in light of its “deeply

revealing nature . . . , its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection.” *Id.* at 320.

* * *

Since *Carpenter*, no Circuit court has had occasion to pass on whether queries of automatic license plate reader databases constitute Fourth Amendment searches in the context of a criminal case, though one concurrence did. *See United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (expressing doubt that ALPR technology will ever reach the point of providing the sort of surveillance data as the cell-site location information at issue in *Carpenter*). And no federal district court has held that the use of ALPR databases violates the Fourth Amendment. *See, e.g.*, *United States v. Cooper*, No. 23-131, 2025 WL 35035, at *4–7 (E.D.L.A. Jan. 6, 2025); *United States v. Martin*, 753 F. Supp. 3d 454, 476 (E.D. Va. 2024); *United States v. Jiles*, No. 8:23-cr-98, 2024 WL 891956, at *19 (D. Neb. Feb. 29, 2024); *United States v. Porter*, No. 21-cr-00087, 2022 WL 124563, at *3 (N.D. Ill. Jan. 13, 2022); *United States v. Rubin*, 556 F. Supp. 3d 1123, 1124 (N.D. Cal. 2021); *United States v. Bowers*, No. 2:18-cr-00292, 2021 WL 4775977, at *3 (W.D. Pa. Oct. 11, 2021); *see also Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1095 (Mass. 2020) (holding that, although an individual has a privacy interest in the whole of his movements, that interest was not implicated by the use of ALPR databases in that case).

In 2021, the Fourth Circuit sitting *en banc* applied *Carpenter* in a civil case and held that warrantless access to an aerial surveillance system (not an automatic license plate reader database) constituted an unconstitutional search under the Fourth Amendment. *Leaders of a Beautiful Struggle v. Baltimore Police Dep’t*, 2 F.4th

330, 333 (4th Cir. 2021) (en banc). Weather permitting, the system in *Leaders of a Beautiful Struggle* surveilled Baltimore residents during almost all daytime hours, capturing an “estimated twelve hours of coverage of around 90% of the city each day.” *Id.* at 334. Despite the light and weather limitations, and although the cameras’ resolution was limited to one pixel per person or vehicle, the Fourth Circuit determined that law enforcement could deduce the “whole of individuals’ movements” from this data. *Id.* at 333–34. The Fourth Circuit based its analysis on *Carpenter*’s delineation “between short-term tracking of public movements . . . and prolonged tracking that can reveal intimate details through habits and patterns.” *Id.* at 341.

II. ALPR Use and the Fourth Amendment

Once one moves beyond the traditional property-based framework of the Fourth Amendment, these competing lines of analysis leave real doubt about the proper analytical framework for use of automatic license plate reader databases. Because of the real-world consequences flowing from the competing approaches, the Supreme Court will ultimately need to address this and other emerging technology to articulate reasonably coherent constitutional principles and to ensure uniform application of a consistent standard.

To illustrate the issues, lower court acceptance of ALPR databases leaves serious doubt about the point, if any, at which governmental use of cameras crosses the line to an impermissible warrantless search and whether linking images to a larger network or enhancing them through the use of artificial intelligence or other emerging technologies leads to a different result. Such surveillance could become too intrusive and run afoul of *Carpenter* at some point. But when? Nor is it clear what

aspect of the technology implicates the Fourth Amendment in the first place. If it is the ongoing operation of the cameras, then many traditional Fourth Amendment doctrines other than *Carpenter* do not appear to have contemplated practices relevantly similar to the one at issue, and even *Carpenter* might not sufficiently secure the rights the Fourth Amendment protects. On the other hand, if a Fourth Amendment search occurs whenever law enforcement queries an ALPR database, then such querying would require a warrant (absent an exception such as exigent circumstances), making this technology like others to which the courts and law enforcement have adapted without too much difficulty.

However those issues and questions ultimately play out, in this case the Court determines that the lines of authority under the Fourth Amendment that govern license plates and the exterior appearance of a vehicle, deriving from the plain-view doctrine control. That is, under Fourth Amendment jurisprudence, Mr. Sturdivant has no reasonable expectation of privacy in the appearance of his vehicle or in his license plate number. Therefore, the query of a database containing this information does not violate Mr. Sturdivant's rights under the Fourth Amendment. *See Ellison*, 462 F.3d 557, 566. Therefore, no search occurred for purposes of the Fourth Amendment. In short, as suggested earlier, the use of automatic license plate reader databases on the facts of this case represent, at most, only a marginal extension of *Ellison* and its predecessors.

Though reasonable people could disagree, in the Court's view, *Carpenter* does not govern the analysis on the facts presented here. For starters, the Supreme Court

framed *Carpenter* as a narrow decision dependent on the “unique nature” of historical cell-site location data. 585 U.S. at 309, 315. It emphasized that it decided only the question before it regarding historical cell-site location information and disturbed no Fourth Amendment precedents. *Id.* at 316. And the Supreme Court noted that it must tread carefully when addressing an emerging technology. *Id.* The question presented addressed historical data that “provide a comprehensive chronicle of [a person]’s past movements.” *Id.* at 300. And the Supreme Court’s holding expressly did not call into question “security cameras” and other “conventional surveillance techniques and tools.” *Id.* at 316.

Admittedly, automatic license plate reader databases are not strictly a conventional surveillance technique or tool. But *Carpenter* does not compel a contrary result in any event. In *Carpenter*, the Supreme Court confronted a surveillance system that provided an average of 101 data points per day, each of which placed an individual within an area ranging from one-eighth to four square miles. 585 U.S. at 312. In this case, the surveillance involves approximately 1,800 to 3,000 cameras in the local area (aggregating the Cuyahoga County Flock and greater Cleveland area ELSAG systems) that ultimately produced at least 26 data points over the course of six weeks, each of which showed the suspect vehicle’s precise location. (ECF No. 92-11; ECF No. 92-17; ECF No. 97-1; ECF No. 97, PageID #1705; ECF No. 98, PageID #1888.) The record does not indicate the total number of results that the system generated, from which law enforcement selected the final 26 images, because law enforcement did not save reports of the search results. However, another

federal court found that Flock’s system shows a maximum of 2,500 results per search. *Martin*, 753 F. Supp. 3d at 459. Here, between December 24 and December 26, 2021, Thrush appears to have run 80 to 90 Flock searches in support of the investigation. (ECF No. 92-13, PageID #1189–91.)

Because of the significant differences between cell-site location information and automatic license plate reader data, direct comparison of these quantitative figures is not necessarily helpful. Defendant argues that automatic license plate reader data can be even more granular and invasive than cell-site location information, and the United States argues the contrary.

In some ways, and on the facts of this case, automatic license plate reader databases are less intrusive than historical cell-site location information. Unlike the “near perfect surveillance” achievable through analysis of historical cell-site location information, the ALPR data in this case could not create “an all-encompassing record” of Mr. Sturdivant’s whereabouts. *Carpenter*, 585 U.S. at 311–12. Unlike a cell phone, a car does not track “nearly exactly the movements of its owner.” *Id.* at 311. Further, there is no indication in the record that law enforcement could recreate the direct path of Mr. Sturdivant’s car, though some of it can be inferred. Even in combination with information from other sources, the ALPR surveillance in this case did not generate enough data for agents to “catalogue every single movement of [his] car.” *Id.* at 310 (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment)). Instead, it provided discrete data points with considerable stretches of obscurity in between. It is true that inference cannot insulate a search from Fourth Amendment

scrutiny. *Id.* at 312. But no amount of inference could create a “detailed log of [Mr. Studivant’s] movements” from the data at issue here. *Id.*

Nor did this surveillance supply the “intimate window” into Mr. Sturdivant’s personal life that worried the Supreme Court in *Carpenter*. *Id.* at 311. Defendant claims that the use of ALPR in this case identified his girlfriend and her residence and even showed “on which nights Mr. Sturdivant stayed overnight there.” (ECF No. 99, PageID #1918.) But there is no evidence in the record indicating that law enforcement used ALPR to deduce Mr. Sturdivant’s overnight locations and thereby identify his girlfriend. Instead, law enforcement appears to have targeted her through conventional investigative means after identifying Mr. Sturdivant as the owner of the suspect vehicle. Nor are the 26 data points at issue in this case dense enough to infer that Mr. Sturdivant stayed at a particular location overnight. Indeed, none was captured before 6:30 a.m. or after 5:30 p.m., and none associates his car with a particular residence. On different facts, law enforcement could use ALPR more invasively to uncover a target’s personal habits or other intimate details. But the Court cannot say that “potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.” *Dow Chem. Co. v. United States*, 476 U.S. 227, 238 n.5 (1986) (quoting *United States v. Karo*, 468 U.S. 705, 712 (1984)).

For all of these reasons, this specific record does not present a privacy threat analogous to the one in *Carpenter*. In some ways, automatic license plate reader data can be more granular than cell-site location information. Rather than placing a vehicle somewhere in a sector up to several square miles large, each ALPR data point

can pinpoint the vehicle’s precise location at a specific time. Because each ALPR search result is a photograph, it supplies richer visual information about the car and its surroundings. And although ALPR photos cannot identify the driver inside the car, common sense dictates that the registered owner of a personal vehicle, or a friend or relative, will usually be the driver of the car.

Moreover, historical cell-site location information and historical automatic license plate reader data both operate retrospectively. Accordingly, law enforcement does not need any advance suspicion to track a vehicle using the information from ALPR databases. Instead, the cameras indiscriminately capture every vehicle that passes them, and officers “can now travel back in time to retrace a [vehicle’s] whereabouts, subject only to the retention policies” of private companies like Flock or, in the case of publicly owned systems, government institutions themselves. *Carpenter*, 585 U.S. at 312. “With enough cameras in enough locations, the historic location data from an ALPR system [could] invade a reasonable expectation of privacy.” *McCarthy*, 142 N.E.3d at 1104.

Because an expectation of privacy must be “one that society is prepared to recognize as reasonable,” *Katz*, 389 U.S. at 361 (Harlan, J., concurring), it feels odd for unelected judges to make such determinations. In the absence of legislative enactments balancing the competing interests, juries might make better decisionmakers and arbiters of reasonableness, particularly in an area of rapid technological change. Whatever the merits of such an approach, the law generally reserves such questions for a court to decide as a matter of law.

Accordingly, the record in this case presents enough significant differences from *Carpenter* that that ruling, in the Court’s view, does not provide the proper analytical framework. To be sure, sophisticated systems like Flock and ELSAG represent “a technological advance” that portends levels of surveillance different in kind from those based on conventional security cameras. *United States v. Brown*, No. 19-cr-949, 2021 WL 4963602, at *3 (N.D. Ill. Oct. 26, 2021). “If the technology evolves” to engender surveillance capabilities comparable to those in *Carpenter*, “then perhaps in the future a warrant may be required.” *Yang*, 958 F. 3d at 864 (Bea, J., concurring). But on the record before it, the Court cannot say that this case presents “dragnet type law enforcement practices” constituting a Fourth Amendment search. See *United States v. Knotts*, 460 U.S. 276, 284 (1983).

However, that day might well be on the horizon. The ALPR surveillance in this case—yielding at least 26 photographs of Mr. Sturdivant’s car over six weeks from an unknown number of total search results—was more extensive than that in many federal cases thus far. Cf. *United States v. Toombs*, 671 F. Supp. 3d 1329, 1334 (E.D. Ala. 2023) (single data point); *United States v. Graham*, No. 21-645, 2022 WL 4132488, at *5 (D.N.J. Sept. 12, 2022) (same); *Yang*, 958 F.3d at 855–56 (two images captured one second apart); *United States v. Porter*, 2022 WL 124563, at *1 (N.D. Ill. Jan. 13, 2022) (two images); *United States v. Mapson*, 96 F.4th 1323, 1334 (11th Cir. 2024) (three locations); *United States v. Rubin*, 556 F. Supp. 3d 1123, 1125 (N.D. Cal. 2021) (“several” results); *Jiles*, 2024 WL 891956, at *3 (“five or six” results); *Brown*, 2021 WL 4963602, at *3 (“about two dozen snapshots” over ten weeks); *Martin*, 753

F. Supp. 3d at 459 (one Flock query returning the maximum of 2,500 results); *but cf.* *Bowers*, 2021 WL 4775977, at *1 (106 results in 33 locations over 4.5 months). Compared to most other cases involving ALPR, the record here shows a qualitative leap forward, placing the evidence generated from such technology at risk in the absence of a warrant.

CONCLUSION

For the foregoing reasons, the Court **DENIES** Defendant's motion to suppress. (ECF No. 92; ECF No. 93.) In doing so, the Court limits its analysis to the facts and record presented. It does not purport to address all possible manifestations of ALPR data searches. After all, "Fourth Amendment cases must be decided on the facts of each case, not by extravagant generalizations." *Dow Chem.*, 476 U.S. at 238 n.5.

SO ORDERED.

Dated: June 9, 2025



J. Philip Calabrese
United States District Judge
Northern District of Ohio